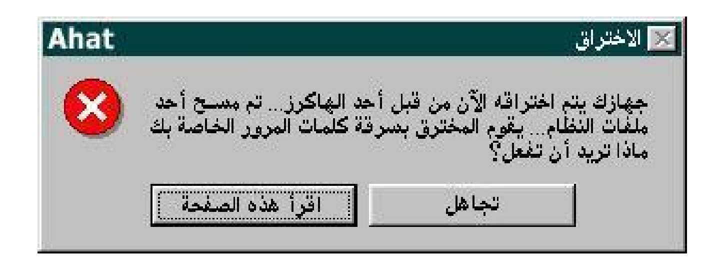
ما هو الاختراق؟



الاختراق بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف.. وحينما نتكلم عن الاختراق بشكل عام فنقصد بذلك قدرة المخترق على الدخول الى جهاز شخص ما بغض النظر عن الأضرار التي قد يحدثها، فحينما يستطيع الدخول الى جهاز آخر فهو مخترق (Hacker) أما عندما يقوم بحذف ملف أو تشغيل آخر أو جلب ثالث فهو مخرب.(Cracker)

كيف يتم الاختراق؟

اختراق الأجهزة هو كأي اختراق آخر لشيءٍ ما.. له طرق وأسس يستطيع من خلالها المخترق التطفل على أجهزة الآخرين عن طريق معرفة الثغرات الموجودة في ذلك النظام.. وغالباً ما تكون تلك الثغرات في المنافذ (Ports) الخاصة بالجهاز... وهذه المنافذ يمكن وصفها بأبسط شكل على أنها بوابات للجهاز على الانترنت.. على سبيل المثال: المنفذ 80 غالباً ما يكون مخصصاً لموفر الخدمة كي يتم دخول المستخدم الانترنت وفي بعض الأوقات يكون المنفذ رقمه 8080 ... هناك طرق عديدة للاختراق أبسطها والتي يمكن للمبتدئين استخدامها هي البرامج التي تعتمد نظام (الزبون/الخادم (client/server) (حيث تحتوي على ملفين أحدهما Serverيرسل إلى الجهاز المصاب بطريقة ما، والآخر Client يتم تشغيله من قبل المخترق للتحكم في الجهاز المصاب وعند تشغيل ملف الـ Server من قبل المُختَرَق يصبح الكمبيوتر عرضة للاختراق حيث يتم فتح أحد المنافذ (Ports) وغالباً ما يكون البورت 12345 أو12346 وبذلك يستطيع الاختراق ببرنامج مخصص لذلك كبرنامج NetBus أو NetSphere أو BackOrifice ويفعل ما يحلو له. كما يستطيع أشخاص آخرون (اضافة الى من وضع الملف في جهازك) فعل نفس الشيء بك حينما يقومون بعمل مسح للبورتات (Port Scanning) فيجدون البورت لديك مفتوح.. هذه الطريقة التي ذكرتها هي أبسط أشكال الاختراق، فهناك طرق عديدة تمكن المتطفلين من اختراقك مباشرة بدون إرسال ملفات! لدرجة أن جمعية للمقرصنين في أميركا ابتكرت طريقة للاختراق متطورة للغاية حيث يتم اختراقك عن طريق حزم البيانات التي تتدفق مع الاتصالات الهاتفية عبر انترنت فيتم اعتراض تلك البيانات والتحكم في جهازك وأنت (يا غافلين لكم الله!!(

كيف تواجه الاختراق؟

يجب أن تعرف في المقام الأول أنك مادمت متصلاً على الشبكة (Online) فأنت معرض للاختراق في أي وقت وبأي طريقة كانت وقد يستهدفك أحد المخترقين (الهاكرز) لسبب ما أو عشوائياً حتى، وربما يكون هذا الهاكر خبيراً (Expert) فيمكنه اختراقك بحيث لا تحس بما يفعله تجاهك !!وعلى هذا فأفضل طريقة هي عدم وضع أشيائك الهامة والخاصة داخل جهازك كرقم بطاقة الإئتمان أو أرقامك السرية، وهناك طريقة أفضل وهي استخدام جهاز خاص للاتصال بالانترنت فقط لا يحتوي على معلومات هامة، وان كانت هذه الطريقة مكلفة بعض الشيء ولكن للضرورة أحكام. هناك برامج مضادة للاختراق ولكن عموماً فهي ليست مضمونة تماماً ولكن لا مانع من استخدامها حيث ستفيدك في التخلص من بعض الهاكرز ولكن ليس الخبراء منهم.. بالنسبة للبرامج التي ذكرتها في البداية والتي تخترق عن طريق إرسال ملف تجسس كملفات (Patch) فلا داعي للخوف منها طالما كنت تمتلك برنامج مضاد جيد للفيروسات كبرنامجي (McAfee Virus Scan Last Update أو(Norton AntiVirus 5.0 Last Update) هذين البرنامجين يؤمنان حماية من ملفات التجسس ويعتبرانها فيروسات لذلك إذا وجد مثل هذه الملفات يقومان بتحذيرك على الفور.. هناك برامج أخرى مخصصة للحماية من الهاكرز فقط كبرنامج LookDown2000 أو NetBuster أو IntruderAlert'99.

نقاط متفرقة

-الانترنت وضعت للإفادة وتبادل المعلومات والثقافات، لذلك فمن غير اللائق استخدامها للتطفل على الآخرين وسرقة معلوماتهم.

-احذر من التباهي بقدرتك على حماية جهازك حماية تامة وبأن جهازك غير قابل للاختراق لأن هناك دائماً من هم أعلم منك وسيعتبرون ذلك تحدياً لهم.

-حاول دائماً تغيير كلمة السر بصورة دورية فهي قابلة للاختراق.

-أي ربط شبكي يترتب عليه مخاطر من الاختراق.. حتى الشبكات المحلية.(Intranet)

-أفضل الطرق للحماية هي جعل عملية الاختراق صعبة ومكلفة للمتطفلين

abdelfatahtei@yahoo.com